02_資安事件及異常紀錄 - 一般 #762

一般 # 790 (Closed-關閉): 內部自行掃描追蹤

192.168.0.4

2024-06-05 10:26 - Joy Liao

狀態:	Closed-關閉	**開始日期:**	2024-06-05
優先權:	Normal	**完成日期:**	
被分派者:	弘政 黃	**完成百分比:**	0%
分類:		**預估工時:**	0:00 小時

概述

Riello NetMan 204 預設憑證 (SSH)
7.5 (高)
100
%
192.168.0.4
22/TCP
2024年5月27日星期一14:06 CST
摘要
遠端 Riello NetMan 204 網路卡使用已知的預設憑證進行 SSH 登入。
檢測結果
可以使用者「admin」身分、密碼「admin」登入並執行「cat /etc/passwd」。結果：

管理員:x:0:0:管理員:/share/homes/admin:/bin/sh
來賓:x:65534:65534:來賓:/share/homes/guest:/bin/sh
httpdusr:x:99:0:Apache httpd **使用者:/tmp:/bin/sh**
[sshd]:x:110:65534:SSHD**權限分離:/var/empty:/bin/sh**
管理員:x:500:100:Linux 使用者,,,:/share/homes/administrator:/bin/sh
檢測方法
嘗試使用已知的預設憑證登入。注意：對於非 Riello
設備，也可能會報告預設的「管理員」和「使用者」憑證。目前這個結果是預期的。
細節：
Riello NetMan 204 預設憑證 (SSH)
OID：1.3.6.1.4.1.25623.1.0.140001
使用版本：
2023-12-20T13:05:58+08:00
影響
遠端攻擊者可能會利用此問題來存取敏感資訊或修改系統配置。
解決方案
解決方案類型：
解決方法
變更受影響帳戶的密碼。
參考
其他
https://www.exploit-db.com/exploits/41208

歷史

#1 - 2024-06-25 09:54 - Joy Liao

- 父議題 設定為 #790

#2 - 2024-11-21 09:53 - Joy Liao

- 狀態 從 New-新增 變更為 Resolved-解決

#3 - 2024-11-21 09:55 - Joy Liao

- 狀態 從 Resolved-解決 變更為 Closed-關閉